SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Lucija Fijan

MATRICE NAD NEKOMUTATIVNIM PRSTENIMA

Diplomski rad

Voditelj rada:
prof.dr.sc.Ozren Perše

Zagreb, 2016.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Za mog djeda Juraja Vutmeja

Sadržaj

Uvod

U mnogim primjenama, modul se dekomponira u direktnu sumu prostih modula, pomoću kojeg se zatim može razviti precizna strukturna teorija. Ovaj rad posvećen je tim rezultatima koji mogu biti općenito dokazani. Koncept prstena se prvi put pojavljuje u pokušaju dokazivanja posljednjeg Fermatov teorema od strane Richarda Dedekinda 1880.-tih godina. Nakon doprinosa drugim poljima matematike, uglavnom teoriji brojeva, ideja prstenova je generalizirana i čvrsto uspostavljena tijekom 1920.-tih godina od Emmy Noether i Wolfganga Krulla. U svrhu istraživanja prstenova, matematičari su osmislili razne pojmove za razlomljivanje prstena u manje, bolje razumljive dijelove poput ideala i prostih prstena. Uz navedene apstraktne pojmovi, teoretičari prstena su također napravili velike razlike između teorije komutativnih prstenova i teorije nekomutativnih prstenova - bivša članica algebarske teorije brojeve i algebarske geometrije. Posebno bogata teorija razvila se iz specijalne klase komutativnih prstenova, poznatih kao polja, koja se nalazi unutar područja teorije polja. Isto tako, iz odgovarajuće teorije nekomutativnih prstenova razvila se teorija od velikog interesa istraživanja teoretičara nekomutativnih prstenova - teorija nekomutativnih prstenova s dijeljenjem.

Opišimo ukratko sadržaj ovog rada. U prvom i drugom poglavlju pod nazivom Prsteni i Moduli uvodimo osnovne pojmove koji su nam potrebni u daljnjem dijelu rada. Pojam poluprostota, kojim se bavimo u trećem poglavlju, je najosnovniji termin koji se proteže kroz čitav diplomski rad. Prezentiramo tri definicije poluprostog modula i dokazujemo da su one ekvivalentne. Pomoću navedenih uvjetima možemo dokazati Jacobsonov teorem o gustoći te definirati pojmove poluprostog i prostog prstena. Uz Jacobsonov teorem u radu dokazujemo i druge važne teoreme, kao primjer Wedderburnov teorem koji nam daje prikaz prstena R kao D-endomorfizam nad modulom E, gdje sa D označavamo konačnodimenzionalnu algebru sa dijeljenjem nad poljem k.

Poglavlje 1

Prsteni

1.1 Osnovni pojmovi

Definicija 1.1.1. *Neprazan skup $G = (G, \cdot)$, gdje je $\cdot : G \times G \longrightarrow G$ binarna operacija zove se **grupa** ako vrijede sljedeća svojstva :*
1) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, za sve $x, y, z \in G$ (asocijativnos)
2) $(\exists e \in G)$ takav da vrijedi $e \cdot x = x \cdot e = x$, za svaki $x \in G$ (neutralni element)
3) Za svaki $x \in G$ postoji jedinstveni $x^{-1} \in G$ takav da vrijedi $x \cdot x^{-1} = x^{-1} \cdot x = e$ (inverzni element)

Element e, ili e_G ako želimo posebno naglasiti da je riječ o grupi G, zove se **neutralni element grupe**, ili kraće **neutral grupe**. Za zadani $x \in G$, element $x^{-1} \in G$ koji zadovoljava gore navedeno treće po redu svojstvo, zove se **inverzni element od** x, ili kraće **inverz od** x. Ako još vrijedi i svojstvo

$$x \cdot y = y \cdot x, \text{ za sve } x, y \in G \text{ (komutativnost)}$$

onda kažemo da je G **komutativna grupa**, a u suprotnom govorimo o **nekomutativnoj grupi**. Ako imamo neki skup G na kojemu je definirana operacija $\cdot : G \times G \longrightarrow G$, tj. za bilo koje $x, y \in G$ je uvijek i $x \cdot y \in G$, kažemo da je $(G, \cdot)$ **grupoid**. Grupoid u kojemu vrijedi i asocijativnost zove se **polugrupa**. Polugrupa koja ima neutralni element zove se **monoid**. Jasno, monoid u kojemu postoji inverz svakog elementa je grupa.

Definicija 1.1.2. *Neprazan skup $R = (R, +, \cdot)$ zovemo **prsten** ukoliko je za operacije zbrajanja $+ : R \times R \to R$ i množenja $\cdot : R \times R \to R$ ispunjeno sljedeće :*
(1) (R,+) je komutativna grupa sa neutralom 0=0_R
(2) (R,·) je polugrupa, tj. množenje je asocijativno.
(3) Vrijedi distributivnost "množenja prema zbrajanju", tj.

$$x \cdot (y + z) = x \cdot y + x \cdot z, \forall x, y, z \in R$$
$$(x + y) \cdot z = x \cdot z + y \cdot z, \forall x, y, z \in R$$

*(4) Postoji **jedinični element**, ili kraće **jedinica**, $1 = 1_R \in R$ takav da je $1 \cdot x = x \cdot 1 = x$, $\forall x \in R$.*

Element $0=0_R$,neutral u grupi $(R,+)$ zovemo **nula** prstena R. Prsten R je **komutativan prsten** ako je $x \cdot y = y \cdot x$, $\forall x, y \in R$. Inače govorimo o **nekomutativnom prstenu**. Osnovna podjela prstena je na komutativne i nekomutativne.

Za svaki prsten R možemo definirati suprotan prsten R^{op}.

Definicija 1.1.3. *Suprotan prsten R^{op} prstena $(R, +, \cdot)$ je prsten $(R^{op}, +, *)$ sa svojstvom*

$$a * b = b \cdot a, \forall a, b \in R$$

Definicija 1.1.4. *Skup $S \subseteq R$, gdje je R neki prsten, je **potprsten** od R ako je $S = (S, +, \cdot)$ i sam prsten. Drugim riječima, S je potprsten od R ako vrijede sljedeća dva uvjeta:*

(1) $(\forall x, y \in S); x - y \in S$ *(tj. $(S,+)$ je grupa)*
(2) $(\forall x, y \in S); x \cdot y \in S$ *(tj. $(S,\cdot)$ je grupoid)*

Činjenicu da je S potprsten od R označavamo, analogno kao i kod grupa, sa $S \leq R$.

Definicija 1.1.5. *Element $0 \neq \lambda \in R$ (tj. $0 \neq \varphi \in R$) takav da je $\lambda x = 0$ (tj. $x\varphi = 0$), za $0 \neq x \in R$ zove se **lijevi** (tj. **desni**) **djelitelj nule**.*

R je **integralna domena**, ili kraće **domena**, ako nema ni lijevih ni desnih djelitelja nule. Element $\omega \in R$ gdje je R prsten, je **invertibilan**, ako $\exists \omega' \in R$ takav da je

$$\omega\omega' = \omega'\omega = 1$$

Koristit ćemo oznaku

$$R^{\times} := \text{grupa invertibilnih elemenata u } R$$

Definicija 1.1.6. *Prsten R je **tijelo**, ili **prsten s dijeljenjem**, ako je svaki ne-nul element u R invertibilan; tojest, ukoliko je*

$$R^{\times} = R \setminus \{0\}.$$

Komutativno tijelo zove se **polje**. Polje k je **algebarski zatvoreno** ako svaki polinom stupnja većeg ili jednakog jedan s koeficijentima iz k ima korijen u k.

Definicija 1.1.7. *Ako su* $(R_\lambda, \lambda \in \Lambda)$ *prsteni,definiramo*

$$\prod_{\lambda\in\Lambda} := \{f : \Lambda \longrightarrow \bigcup_\lambda R_\lambda | f(\lambda) \in R_\lambda\}$$

sa zbrajanjem i množenjem "po komponentama"

$$(f + g)(\lambda) := f(\lambda) + g(\lambda) \; i \; (f \cdot g)(\lambda) := f(\lambda) \cdot g(\lambda);$$

tako je dobiven prsten $(\prod_{\lambda\in\Lambda} R_\lambda, +, \cdot)$*, koji se zove* ***direktan produkt prstena*** $(R_\lambda)_\Lambda$*. Potprsten*

$$\bigoplus_{\lambda\in\Lambda} R_\lambda := \{f \in \prod_{\lambda\in\Lambda} R_\lambda | f(\lambda) \neq 0_\lambda \text{ za konačno mnogo } \lambda \in \Lambda\}$$

direktnog produkta $(\prod_{\lambda\in\Lambda} R_\lambda)$*, zove se* ***direktna suma prstena*** $(R_\lambda)_\Lambda$*; jasno, ovdje je sa* 0_λ *označen neutral za zbrajanje u grupi* $(R_\lambda, +)$*.*

1.2 Homomorfizam prstena

Definicija 1.2.1. *Neka su R i S dva prstena. Preslikavanje* $f : R \to S$ *nazivamo* ***homomorfizam prstena*** *ukoliko je aditivno i multiplikativno, tj. ako vrijedi* $f(x + y) = f(x) + x(y)$ *i* $f(xy) = f(x)f(y)$ *,* $\forall x,y \in R$ *te ako je* $f(1_R) = 1_S$*.*

Sa $\mathrm{Hom}(R, S)$ označavamo skup svih homomorfizma sa R u S. Homomorfizam f koji je još i injekcija nazivamo **monomorfizam**, f koji je i surjekcija zovemo **epimorfizam**. Bijektivan homomorfizam zovemo **izomorfizam**. Za dva prstena R i S reći ćemo da su izomorfni ako postoji neki izomorfizam f među njima; tu činjenicu označavamo sa

$$R \cong S.$$

Definicija 1.2.2. *Neka su R i S dva prstena.* ***Anti-izomorfizam*** *između prstena R i S je izomorfizam između prstena R i* S^{op} *(ili ekvivalentno* R^{op} *i S).*

Za dva prstena R i S reći ćemo da su anti-izomorfni ako postoji neki anti-izomorfizam među njima.

Posebno, ako je $R = S$, tj. ako imamo homomorfizam $f : R \to R$, onda kažemo da je f **endomorfizam** od R. Sa $\mathrm{End}\ R$ označavat ćemo skup svih endomorfizma od R.
Endomorfizam koji je još i bijekcija zove se **automorfizam** od R. Sa $\mathrm{Aut}\ R$ označavamo skup svih automorfizma od R.

Za proizvoljan homomorfizam $f : R \to S$ definiramo njegovu **jezgru**

$$\mathrm{Ker} f := f^{-1}(\{0_S\}) = \{x \in R | f(x) = 0_S\}$$

i njegovu **sliku**

$$\text{Im } f: = f(S) = \{f(x)|x \in S\}$$

1.3 Primjeri nekomutativnih prstena

(1) *Prsten matrica*

$$M_n(K) = \{(x_{ij})|x_{ij} \in K\}$$

reda n-puta-n sa keficijentima iz nekog polja K=$\mathbb{C}$,$\mathbb{R}$,$\mathbb{Q}$...; to je prsten uz standardno množenje i zbrajanje matrica. Jedinica u tom prstenu je I=I_n, dok je neutral za zbrajanje nul-matrica O, matrica koja svuda ima 0. Nadalje,

$$M_n(K) \text{ je integralna domena} \Longleftrightarrow n = 1.$$

Primijetimo ovdje da je karakteristika

$$\text{char } M_n(K) = \text{char (K)},$$

te da je skup invertibilnih elemenata $M_n(K)$ jednak

$$M_n(K)^\times = GL_n(K).$$

Napomenimo ovdje kako ćemo u ovom radu promatrati prstene M_n(R), n-puta-n matrica sa koeficijentima iz nekog, ne nužno komutativnog, prstena$R$.

(2) Promatrajmo sada vektorski prostor E nad K i skup svih linearnih preslikavanja $E \longrightarrow E$, $EndE = End_K E$. Ako na tom skupu defniramo *zbrajanje* "po točkama"

$$(f + g)(e) := f(e) + g(e), \forall f, g \in EndE$$

te *množenje* kao kompoziciju fukcija

$$EndE \times EndE \ni (f, g) \longmapsto fg := f \circ g \in EndE$$

onda je $EndE$ nekomutativan prsten. Sada možemo definirati grupu invertibilnih elemenata od $EndE$ sa

$$GL(E) = (EndE)^\times$$

(3) Neka je G proizvoljna grupa i neka je R proizvoljan prsten. Definirajmo skup

$$R[G] = \{\varphi : G \longrightarrow R|\varphi(g) \neq 0 \text{ za konačno mnogo } g \in G\} = \{\textstyle\sum_{i=1}^n r_i g_i | r_i \in R, g_i \in G\}$$

te na njemu promatramo operaciju *zbrajanja* "po komponentama"

$$(\varphi + \psi)(g) := \varphi(g) + \psi(g), \forall g \in G.$$

Tako je zapravo $(R[G], +)$ aditivna grupa izomorfna direktnoj sumi od card G primjeraka aditivne grupe $(R, +)$, tj.

$$(R[G], +) \cong \oplus_{g \in G}(R, +).$$

Sada na $R[G]$ definirajmo i operaciju množenja ovako:

$$(\sum_{i=1}^{m} r_i g_i) * (\sum_{j=1}^{n} s_j h_j) := \sum_i \sum_j (r_i s_j) g_i h_j.$$

Tojest, ako elemente koje množimo zapišemo kao funkcije

$$\varphi = \sum_{g \in G} r_g g \text{ i } \psi = \sum_{h \in G} s_h h$$

gdje je samo konačno mnogo r_g i s_h različito od 0, onda je

$$(\varphi * \psi)(x) := \sum_{(g,h) \in G \times G, gh = x} \varphi(g)\psi(h) = \sum_{(g,h) \in G \times G, gh = x} r_g s_s$$

množenje $(\varphi, \psi) \mapsto \varphi * \psi$,za $\varphi, \psi : G \longrightarrow R$ zove se **konvolucijsko množenje**. Sada je lako provjeriti da je

$$R[G] = (R[G], +, *)$$

prsten; on se zove **grupni prsten**, za G i R.
Jedinica u tom prstenu je $\varepsilon = 1e$, tj. funkcija

$$\varepsilon : G \longrightarrow R, \varepsilon(x) = \begin{cases} 1, & x = e \\ 0, & \text{inače} \end{cases}$$

jasno, e je neutral u grupi G.
Primijetimo da za grupu G te prstene R i $R[G]$ imamo

$$R[G] \text{ komutativan} \Leftrightarrow G \text{ komutativna i } R \text{ komutativan.}$$

Poglavlje 2

Moduli

2.1 Osnovni pojmovi

Definicija 2.1.1. *Neka je R prsten.* ***Lijevi R-modul*** *je aditivna Abelova grupa M s funkcijom $R \times M \to M$ (koju zovemo djelovanje i za koju označavamo $(r, m) \mapsto rm$) takvom da za sve r, s ∈ R i sve m, n ∈ M vrijedi :*
(1) $r(m + n) = rm + rn$
(2) $(r + s)m = rm + sm$
(3) $r(sm) = (rs)m$
Ako ima jedinicu 1_R vrijedi i
(4) $1_R m = m$ za sve m∈M onda kažemo da je M jedinični R-modul.

Ako je R prsten s dijeljenjem onda unitalni lijevi R-modul zovemo **lijevi vektorski prostor**. Strukturu **desnog R-modula** na Abelovoj grupi definiramo analogno funkcijom $M \times R \to M$.

U daljnjem tekstu svi rezultati se odnose na lijeve R-module koje ćemo jednostavno nazivati R-moduli. Analogni rezultati vrijede za desne R-module.

Definicija 2.1.2. *Neka je R prsten i neka je M R-modul. Za S podskup od M kažemo da je* ***R-linearno zavisan*** *ako postoje međusobno različiti $x_1, ..., x_n$ iz S i elementi $a_1, ..., a_n$ iz R, koji nisu svi jednaki 0, takvi da*

$$a_1 x_1 + ... + a_n x_n = 0$$

Za skup koji nije R-linearno zavisan kažemo da je ***R-linearno nezavisan****.*

Definicija 2.1.3. *Neka je M R-modul. Podskup S od M je* ***baza od*** *M ako S generira M kao R-modul i ako je S R-linearno nezavisan.*

Drugim riječima, $S \subseteq M$ je baza ako i samo ako je
1) $M = \{0\}$ pa je $S = \emptyset$ baza; ili
2) $M \neq \{0\}$ pa je $S \subseteq M$ baza od M ako i samo ako svaki $x \in M$ možemo jedinstveno napisati kao $x = a_1x_1 + ... + a_nx_n$, za $x_1, ..., x_n \in S$ i $a_1, ..., a_n \in R$.

Definicija 2.1.4. *R-modul M je **slobodan** R-modul ako ima bazu.*

Definicija 2.1.5. *Neka je M modul nad R. Neprazan podskup $N \subseteq M$ je **podmodul** od M ako vrijedi :*

(1) $a - b \in N$, za sve a,b $\in N$
(2) $ra \in N$, za sve $a \in N, r \in R$

Ako je M R-modul, $v \in M$ tada skup

$$Rv = \{av : a \in R\}$$

zovemo **lijevi podmodul** od M generiran s v.

Neka je M $R-$modul i N podmodul. Definirat ćemo strukturu modula na kvocijentnom skupu $M/N = \{x + N : x \in M\}$ pri čemu je $x + N = \{x + a : a \in N\}$ klasa od N u M sa zbrajanjem $(x + N) + (y + N) = (x + y) + N$. Neka je $r \in R$. Definiramo $r(x + N)$ kao klasu od $rx + N$. Može se pokazati su navedene operacije dobro definirane, odnosno ne ovise o predstavniku klase. Ove operacije zadovoljavaju aksiome modula na skupu M/N kojeg nazivamo **kvocijentni modul**.

Podmoduli komutativnog prstena R su upravo **ideali**.
Ako je R nekomutativan prsten tada se lijevi R-podmoduli od R nazivaju **lijevi ideali**, a desni podmoduli se nazivaju **desni ideali**. Ideal koji je i lijevi i desni ideal od R naziva se **obostrani ideal**.

Definicija 2.1.6. *Ne-nul modul M se naziva **prost** ako su jedina dva podmodula od M 0 i M.*

Definicija 2.1.7. *Neka je S neprazan podskup R-modula M. Najmanji podmodul od M koji sadrži skup S nazivamo **podmodul generiran skupom S** i označavamo sa (S). Ako je $S = \{x_1, x_2, ..., x_n\}$, tada koristimo oznaku $(S) = (x_1, x_2, ..., x_n)$*

Definicija 2.1.8. *Neka su $N_1, ..., N_k$ podmoduli R-modula M. Podmodul generiran unijom $\bigcup_{i=1}^{k} N_i$ nazivamo suma podmodula N_i i označavamo s $\sum_{i=1}^{k} N_i$.*

Prema ovoj definiciji je

$$(\bigcup_{i=1}^{k} N_i) = \sum_{i=1}^{k} N_i.$$

Ako je $M = \sum_{i=1}^{k} N_i$, M je *generiran podmodulima* N_i.

Definicija 2.1.9. *Neka su $N_1, ..., N_k$ podmoduli R-modula M. Suma podmodula $\sum_{i=1}^{k} N_i$ naziva se **direktna suma** ako se svaki element $x \in \sum_{i=1}^{k} N_i$ može na jedinstven način zapisati kao $x = \sum_{i=1}^{k} x_i$, $x_i \in N_i$. Direktnu sumu označavamo s*

$$N_1 \oplus N_2 \oplus ... \oplus N_k.$$

Ako direktna suma generira cijeli modul M, tada pišemo

$$M = N_1 \oplus N_2 \oplus ... \oplus N_k.$$

Definicija 2.1.10. *Neka je R prsten i neka su $(M_i, i \in I)$ R-moduli. Direktan produkt modula M_i, oznaka $\prod_{i \in I} M_i$, se sastoji od svih familija $(a_i, i \in I)$, $a_i \in M_i$. Zbrajanje je definirano sa $(a_i) + (b_i) = (a_i + b_i)$, a množenje skalarom sa $r(a_i) = (ra_i)$.*

U slučaju konačnog broja modula, lagano se vidi da su pojmovi direktne sume i direktnog produkta ekvivalentni.

Primjeri modula:
(1) R je modul nad samim sobom
(2) Aditivna grupa koja se sastoji samo od 0 je modul nad svakim prstenom
(3) Svaki lijevi ideal od R je modul nad R
(4) $M_n(F)$ je modul nad poljem F i nad prstenom $M_n(F)$

2.2 Homomorfizam modula

Neka su M, N (lijevi) moduli nad prstenom R. Kažemo da je preslikavanje $f : M \to N$ **homomorfizam** R-modula ako za sve $m, n \in M$ i $r \in R$ vrijedi

$$f(m + n) = f(m) + f(n)$$
$$f(rm) = rf(m)$$

Ako želimo da se homomorfizam f odnosi na prsten R, još kažemo da je f R-homomorfizam ili R-linearno preslikavanje. M je **bimodul** nad R ako je M desni i lijevi modul nad R (lijevo i desno množenje ne mora biti isto).

Skup svih homomorfizma $f : M \longrightarrow N$ označavamo sa $Hom_R(M, N)$. Ako je $M = N$, tada kažemo da je f endomorfizam modula M. Skup svih endomorfizama modula M označavamo s $End_R(M)$. Jezgra homomorfizma

$$Kerf = \{x \in M | f(x) = 0\}$$

je podmodul modula M, a slika homomorfizma

$$Imf = \{f(x) | x \in M\}$$

je podmodul modula N. Homomorfizam $f : M \longrightarrow N$ je injekcija ako i samo ako je $Kerf = 0$. Ako je homomorfizam $f : M \longrightarrow N$ bijekcija, tada kažemo da je f izomorfizam modula. U tom slučaju su moduli M i N izomorfni i pišemo $M \simeq N$. Preslikavanje $\varphi : M \longrightarrow M/N$,

$$\varphi(x) = x + N$$

naziva se prirodno preslikavanje. Zbog definicije kvocijentnog modula M/N prirodno preslikavanje je očito homomorfizam iz modula M na modul M/N, tj. preslikavanje $x \longrightarrow x+N$ je homomorfizam modula.

Definicija 2.2.1. *Neka je R komutativan prsten te neka su E i F moduli.* ***Bilinearno preslikavanje***

$$g : E \times E \longrightarrow F$$

je preslikavanje takvo da za dani $x \in E$, preslikavanje $y \longrightarrow g(x, y)$ je R-linearno i za dani $y \in F$, preslikavanje $x \longrightarrow g(x, y)$ je R-linearno preslikavanje. ***R-algebra*** *je modul sa bilinearnim preslikavanjem $g : E \times E \longrightarrow F$.*

Jedna od glavnih podjela algebri je na *komutativne* i *nekomutativne* algebre, gdje je algebra $R = (R, +, \cdot)$ komutativna ukoliko je operacije " $\cdot$ " na R komutativna, a inače je R nekomutativna. Druga podjela algebri, u važnom slučaju kada je A štoviše polje, je na konačnodimenzionalne i beskonačnodimenzionalne algebre. Jasno, u rečenom slučaju je svaka A-algebra R posebno i vektorski prostor nad A, pa je onda dimenzija algebre dobro definirana; naime $dimR = dim_A R$ je standardna dimenzija A-vektorskog prostora R.

Poglavlje 3

Matrice nad nekomutativnim prstenom

3.1 Matrice nad nekomutativnim prstenom

Definicija 3.1.1. *Neka je K nekomutativan prsten. Pod matricom $m \times n$ nad K smatramo dvostruko indeksiranu familiju sa elementima iz K, (a_{ij}), (i=1,...m,j=1,...,n), zapisanu u formi*

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ & \dots & \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$$

Zbrajanje, množenje skalarom te množenje se definiraju na standardni način. Za matrice iste veličine definiramo **zbrajanje po komponentama** . Neka su $A = (a_{ij})$ i $B = (b_{ij})$ matrice iste veličine tada definiramo matricu $A + B$ čija je ij-komponenta jednaka

$$a_{ij} + b_{ij}.$$

Množenje matrica definiramo pod određenim uvjetom. Ako je matrica $A = (a_{ij})$ reda (m, n) te matrica $B = (b_{ij})$ reda (n, r), tj. ako je broj redaka matrice A jednak broju stupaca matrice B tada definiramo matricu AB reda (m, r) čija je ik - komponenta jednaka

$$\sum_{j=1}^{n} a_{ij} b_{jk}$$

Kvadratne matrice nad K formiraju prsten (oznaka $Mat_n(K)$) te postoji dijagonalni homomorfizam prstena $K \to Mat_n$(K).

Neka je R prsten te neka su

$$E = E_1 \oplus ... \oplus E_n \text{ te } F = F_1 \oplus ... \oplus F_m$$

R-moduli izraženi kao direktne sume R- podmodula. Zelimo opisati općeniti R-homomorfizam $E \to F$. Pretpostavimo prvo da F ima samo jednu komponentu $F = F_1$. Neka je

$$\varphi : E_1 \oplus ... \oplus E_n \to F$$

homomorfizam. Neka je $\varphi_j : E_j \to F$ restrikcija preslikavanja φ na E_j. Svaki element $x \in E$ ima jedinstveni prikaz $x = x_1 + ... + x_n, x_j \in E_j$, pa elementu x možemo pridružiti vektor stupac $(x_1, ..., x_n)^t, x_1 \in E_1, ..., x_n \in E_n$. Homomorfizmu φ možemo pridružiti vektor-redak $(\varphi_1, ..., \varphi_n)$, $\varphi_j \in Hom_R(E_j, F)$. Djelovanje φ na $x \in E$ opisano je matričnim množenjem vektor-retka i vektor-stupca.

Općenito, razmatramo homomorfizam

$$\varphi : E_1 \oplus ... \oplus E_n \to F_1 \oplus ... \oplus F_m.$$

Neka je $\pi_i : F_1 \oplus ... \oplus F_m \longrightarrow F_i$ projekcija na i-ti faktor. Tada možemo primijeniti predhodnu primjedbu na $\pi_i \circ \varphi$, za svaki i, tj. postoje jedinstveni $\varphi_{ij} \in Hom_R(E_j, F_i)$ takvi da φ ima matrični prikaz u obliku

$$M(\varphi) = \begin{pmatrix} \varphi_{11} & \cdots & \varphi_{1n} \\ & \cdots & \\ \varphi_{m1} & \cdots & \varphi_{mn} \end{pmatrix}$$

čije je djelovanje na x dano matričnim množenjem

$$\begin{pmatrix} \varphi_{11} & \cdots & \varphi_{1n} \\ & \cdots & \\ \varphi_{m1} & \cdots & \varphi_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Obrnuto, promatrajući matricu φ_{ij} sa $\varphi_{ij} \in Hom_R(E_j, F_i)$ možemo definirati element od $Hom_R(E, F)$ pomoću te matrice. Imamo izomorfizam aditivnih grupa između $Hom_R(E, F)$ i navedene grupe matrica.
Posebno, neka je E fiksni R-modul i $K = End_R(E)$. Tada imamo izomorfizam prstenova

$$End_R(E^{(n)}) \longrightarrow Mat_n(K)$$

koji svakom $\varphi \in End_R(E^{(n)})$ pridružuje matricu

$$\begin{pmatrix} \varphi_{11} & \cdots & \varphi_{1n} \\ & \cdots & \\ \varphi_{m1} & \cdots & \varphi_{mn} \end{pmatrix}$$

određenu kao i prije, djelujući slijeva na vektore-stupce iz $E^{(n)}$ sa komponentama iz E.

Napomena: Neka je E 1-dimenzionalan vektorski prostor nad prstenom dijeljenja D te neka je $\{v\}$ baza. Za svaki $a \in D$ postoji jedinstveno D-linearno preslikavanje $f_a : E \to E$ takvo da je $f_a(v) = av$. Tada imamo pravilo

$$f_a f_b = f_{ba}$$

Tako kad povezujemo matrice sa linearnim preslikavanjem, u ovisnosti o bazi, množenje biva zakrenuto. Unatoč tome, tvrdnja prije ove napomene je točna! Razlog tome je to što smo uzeli φ_{ij} iz $End_R(E)$, a ne iz D (gdje je u ovom slučaju $R = D$). Zato K nije izomorfno sa D (u nekomutativnom slučaju) već anti-izomorfno. Ovo je jedina razlika između formalne elementarne teorije linearnih preslikavanja u komutativnom i nekomutativnom slučaju.

Prisjetimo se da je R-modul E prost ako je različit od 0 te ako nema niti jedan podmodul različit od 0 ili od E.

Propozicija 3.1.2. ***(Schurova lema)*** *Neka su E i F prosti R-moduli. Svaki ne-nul homomorfizam $E \longrightarrow F$ je izomorfizam. Prsten $End_R(E)$ je prsten s dijeljenjem.*

Dokaz. Neka je $f : E \longrightarrow F$ ne-nul homomorfizam. Njegova jezgra i slika su podmoduli, stoga je $Kerf = 0$ i $Imf = E$ pa je f izomorfizam. Ako je $E = F$ tada postoji i inverz od f. □

Sljedeća propozicija u potpunosti opisuje prsten endomorfizma direktnih suma prostih modula.

Propozicija 3.1.3. *Neka je $E = E_1^{(n_1)} \oplus ... \oplus E_r^{(n_r)}$ direktna suma prostih modula, E_i su ne-izomorfni te se svaki ponavlja n_i puta u sumi. Tada, do na permutaciju, $E_1, ..., E_r$ su jedinstveno određeni do na izomorfizam te su multipliciteti $n_1, ...n_r$ jedinstveno određeni. Prsten $End_R(E)$ je izomorfan sa prstenom matrica, tipa*

$$\begin{pmatrix} M_1 & & \dots & 0 \\ 0 & M_2 & & \vdots \\ \vdots & & \ddots & \vdots \\ 0 & & \dots & M_r \end{pmatrix}$$

gdje je M_i $n_i \times n_i$ matrica nad $End_R(E_i)$. (izomorfizam je s obzirom na dekompoziciju u direktnu sumu).

Dokaz. Pretpostavimo da imamo dva R-modula, sa dekompozicijom u direktnu sumu prostih podmodula te izomorfizam

$$E_1^{(n_1)} \oplus ... \oplus E_r^{(n_r)} \longrightarrow F_1^{(m_1)} \oplus ... \oplus F_s^{(m_s)}$$

tako da su E_i ne-izomorfni i F_j ne-izomorfni. Iz Propozicije 2.1.2, zaključujemo da je svaki E_i izomorfan sa nekim F_j i obrnuto. Slijedi da je $r = s$ i, nakon permutacije, $E_i \approx F_i$. Nadalje, izomorfizam mora inducirati izomorfizam

$$E_i^{(n_i)} \longrightarrow F_i^{(m_i)}$$

za svaki i. Kako je $E_i \approx F_i$ bez smanjenja općenitosti možemo pretpostaviti $E_i = F_i$. Sada smo se sveli na dokazivanje: Ako je modul izomorfan sa $E^{(n)}$ i sa $E^{(m)}$, za neki prost modul E, tada je $m = n$. Ali $End_R(E^{(n)})$ je izomorfan sa $n \times n$ prstenom matrica nad prstenom dijeljenja $End_R(E) = K$. Nadalje, taj izomorfizam je izomorfizam K-vektorskih prostora. Dimenzija prostora $n \times n$ matrica nad K je n^2. To dokazuje da je multiplicitet n jedinstveno određen te dokazuje našu propoziciju. □

3.2 Uvjeti koji definiraju poluprostotu

Neka je R prsten. Ako nije drugačije specificirano u ovom poglavlju svi moduli i homomorfizmu su R-moduli i R-homomorfizmi.

Sljedeći uvjeti za modul E su ekvivalentni :
1) E je suma familije prostih podmodula.
2) E je direktna suma familije prostih podmodula.
3) Svaki podmodul F od E je direktni sumand, tj. postoji podmodul F' takav da vrijedi $E = F \oplus F'$.

Sada ćemo dokazati da su ta tri uvjeta ekvivalentna:

Lema 3.2.1. *Neka je $E = \sum_{i \in I}$ suma (ne nužno direktna) prostih podmodula. Tada postoji podskup $J \subset I$ takav da je E direktna suma $\oplus_{j \in J} E_j$.*

Dokaz. Neka je J maksimalni podskup od I takav da je suma $\sum_{j \in J}$ direktna. Tvrdimo da je ta suma jednaka E. Dovoljno je za dokazati da je svaki E_i sadržan u sumi. Ali presjek sume sa E_i je podmodul od E_i, dakle jednak 0 ili E_i. Ako je jednak 0 onda J nije maksimalan jer mu onda možemo pridružiti i. Prema tome E_i je sadržan u sumi pa je naša lema dokazana. □

Lema pokazuje da 1) povlači 2). Da dokažemo da 2) povlači 3) uzimamo podmodul F te neka je J maksimalni podskup od I takav da je suma $F + \oplus_{j \in J} E_j$ direktna. Sličnim zaključivanjem kao prije slijedi da je suma jednaka E.
Konačno, pretpostavimo da vrijedi 3). Da dokažemo da vrijedi 1) prvo ćemo dokazati da

svaki ne-nul podmodul od E sadrži prost podmodul. Neka je $v \in E, v \neq 0$. Tada prema definiciji, Rv je glavni podmodul i jezgra homomorfizma

$$R \longrightarrow Rv$$

je lijevi ideal $L \neq R$. Prema tome L je sadržan u maksimalnom lijevom idealu $M \neq R$. Tada je M/L maksimalni podmodul od R/L (različit od R/L) pa je Mv maksimalni podmodul od Rv, različit od Rv, on odgovara M/L pri izomorfizmu

$$R/L \longrightarrow Rv$$

Možemo pisati $E = Mv \oplus M'$ gdje je M' neki podmodul. Tada vrijedi

$$Rv = Mv \oplus (M' \cap Rv)$$

zbog toga jer se svaki element $x \in Rv$ može jedinstveno zapisati kao suma $x = \alpha v + x'$ sa $\alpha \in M$ i $x' \in M'$ te $x' = x - \alpha v$ leži u Rv. Kako je Mv maksimalan u Rv slijedi da je $M' \cap Rv$ prost, kako smo i htjeli.
Neka je E_0 podmodul od E koji je suma svih prostih podmodula od E. Ako je $E_0 \neq E$ tada je $E = E_0 \oplus F$ sa $F \neq 0$ te postoji prost podmodul od F, što je kontradikcija sa time kako smo definirali E_0 . Ovo dokazuje da 3) povlači 1).

Modul E koji zadovoljava gornja tri uvjeta se naziva **poluprost**.

Propozicija 3.2.2. *Svaki podmodul i svaki kvocijentni modul poluprostog modula je poluprost.*

Dokaz. Neka je F podmodul i F_0 suma svih prostih podmodula od F. Neka je $E = F_0 \oplus F_0^{'}$. Svaki element x iz F ima jedinstveni prikaz u obliku $x = x_0 + x_0^{'}$, $x_0 \in F_0$ i $x_0^{'} \in F_0^{'}$. Ali $x_0^{'} = x - x_0 \in F$ pa je prema tome F direktna suma

$$F = F_0 \oplus (F \cap F_0^{'}).$$

Prema tome mora vrijediti $F_0 = F$ koji je poluprost. Što se tiče kvocijentog modula zapišemo $E = F \oplus F^{'}$. Tada je $F^{'}$ suma svojih prostih podmodula i kanonsko preslikavanje $E \longrightarrow E/F$ inducira izomorfizam $F^{'} \longrightarrow E/F$. Prema tome E/F je poluprost. □

3.3 Teorem o gustoći

Neka je E poluprost R-modul i $R' = R'(E)$ prsten $End_R(E)$. Tada je E također R'-modul, a djelovanje od R' na E je dano sa

$$(\varphi, x) \longrightarrow \varphi(x)$$

$\varphi \in R'$ i $x \in E$. Svaki $\alpha \in R$ inducira R'-homomorfizam $f_\alpha : E \longrightarrow E$ definirano kao $f_\alpha(x) = \alpha x$. Uz takvu definiciju vrijedi:

$$\varphi(\alpha x) = \alpha\varphi(x).$$

Neka je $R'' = R''(E) = End_{R'}(E)$. R' nazivamo **komutant** od R, a R'' nazivamo **bikomutant**. Sada dobivamo homomorfizam prstena

$$R \longrightarrow End_{R'}(E) = R''(E) = R''$$

sa $\alpha \longrightarrow f_\alpha$. Sada se pitamo koliko je velika slika navedenog homomorfizma prstena. Teorem o gustoći nam govori da je slika poprilično velika.

Lema 3.3.1. *Neka je E poluprost modul nad R te neka je $R' = End_R(E)$, $f \in End_{R'}(E)$ kao i predhodno navedeno. Neka je $x \in R$. Tada postoji element $\alpha \in R$ takav da je $\alpha x = f(x)$.*

Dokaz. Kako je E poluprost možemo ga zapisati u obliku R-direktne sume

$$E = Rx \oplus F$$

gdje je F neki podmodul. Neka je $\pi : E \longrightarrow Rx$ projekcija. Tada je $\pi \in R'$ te vrijedi

$$f(x) = f(\pi x) = \pi f(x).$$

Ovo pokazuje da je $f(x) \in Rx$, tj. dokazali smo lemu. □

Teorem o gustoći generalizira lemu uzimajući u obzir konačan broj elemenata iz E umjesto samo jednog. Za dokaz koristimo dijagonalni trik.

Teorem 3.3.2. ***(Jacobson)*** *Neka je E poluprost modul prstena R te neka je $R' = End_R(E)$. Neka je $f \in End_{R'}(E)$ i $x_1, ..., x_n \in E$. Tada postoji element $\alpha \in R$ takav da vrijedi*

$$\alpha x_i = f(x_i), i = 1, ..., n.$$

Ako je E konačno generiran nad R'tada je prirodno preslikavanje $R \longrightarrow End_{R'}(E)$ surjekcija.

Dokaz. Prvo ćemo dokazati teorem u slučaju kada je E prost. Neka je $f^{(n)} : E^{(n)} \longrightarrow E^{(n)}$ produktno preslikavanje takvo da vrijedi

$$f^{(n)}(y_1, ..., y_n) = (f(y_1), ..., f(y_n)).$$

Neka je $R'_n = End_R(E^{(n)})$. Tada je R'_n prsten matrica sa koeficijentima iz R'. Kako f komutira sa elementima iz R' prilikom njegovog djelovanja na E vidimo da je $f^{(n)} \in End_{R'_n}(E^{(n)})$. Prema prethodnoj lemi, postoji element $\alpha \in R$ takav da vrijedi

$$(\alpha x_1, ..., \alpha x_n) = (f(x_1), ..., f(x_n))$$

što smo i htjeli dokazati.
U slučaju kada E nije prost, pretpostavit ćemo da je E jednak konačnoj direktnoj sumi prostih podmodula E_i (ne-izomorfnih) sa multiplicitetima n_i :

$$E = E_1^{(n_1)} \oplus ... \oplus E_r^{(n_r)}, (E_i \not\approx E_j \text{ ako je } i \neq j).$$

Tada matrice koje reprezentiraju prsten endomorfizma se podijele u blokove koji odgovaraju ne-izomorfnim prostim komponentama u našoj dekompoziciji u direknu sumu. Sada ponovno koristimo argument kao i prije. Poanta je da $f^{(n)}$ leži u $End_{R'_n}(E^{(n)})$ te da možemo upotrijebiti lemu.

Ako je E konačno generiran nad R' tada je element $f \in End_{R'}(E)$ određen vrijednostima na konačnom broju elemenata od E iz čega slijedi surjektivnost preslikavanja $R \longrightarrow End_{R'}(E)$. U sljedećim primjenama E je konačnodimenzionalan vektorski prostor nad poljem k te je R k-aglebra pa su prema tome uvjeti konačnosti automatski zadovoljeni.

Argument kada je E beskonačna direktna suma je sličan predhodnom, ali sa različitom notacijom. Međutim, u primjenama ovaj teorem ćemo razmatrati samo u slučaju kada je E konačna direktna suma prostih modula što nam upravo dokazuje sljedeći teorem. □

Korolar 3.3.3. ***(Burnsideov teorem)****. Neka je E konačnodimenzionalan vektorski prostor nad algebarski zatvorenim poljem k te neka je R podalgebra od $End_k(E)$. Ako je E prost R-modul tada je $R = End_{R'}(E)$.*

Dokaz. Tvrdimo da je $End_R(E) = k$. U svakom slučaju $End_R(E)$ je prsten s dijeljenjem R' koji sadrži k kao potprsten i svaki element iz k komutira sa svakim elementom iz R'. Neka je $\alpha \in R'$. Tada je $k(\alpha)$ polje. Nadalje, R' je sadržan u $End_k(E)$ kao k-potprostor pa je prema tome konačnodimenzionalan nad k. Dakle $k(\alpha)$ je konačno nad k pa je jednako k, kako je k algebarski zatvoren. To dokazuje da je $End_R(E) = k$. Neka je sad $\{v_1, ..., v_n\}$ baza od E nad k. Neka je $A \in End_k(E)$. Prema teoremu o gustoći postoji $\alpha \in R$ takav da vrijedi

$$\alpha v_i = A v_i, i = 1, ..., n.$$

Kako je djelovanje od A određeno svojim djelovanjem na bazi zaključujemo da je $R = End_k(E)$.

□

Navedeni korolar se koristi u sljedećoj situaciji: Neka je E konačnodimenzionalan vektorski prostor nad k. Neka je G podmonoid od $GL(E)$ (multiplikativan). G-invarijantan podskup F od E je podskup za kojeg vrijedi $\sigma F \subset F$ za sve $\sigma \in G$. Kažemo da je $E \neq 0$ G**-prost** ako nema niti jedan G-invarijantan podskup osim 0 i sebe samog. Neka je $R = k[G]$ podalgebra od $End_k(E)$ generirana od G nad k. Kako smo pretpostavili da je G monoid slijedi da se R sastoji od linearnih kombinacija

$$\sum a_i \sigma_i \, , a_i \in k \, , \sigma_i \in G.$$

Vidimo da je potprostor F od E G-invarijantan ako i samo ako je R-invarijantan. Prema tome E je G-prost ako i samo ako je prost nad R. Sada možemo ponovno iskazati Burnsideov teorem na sljedeći način:

Korolar 3.3.4. *Neka je E konačnodimenzionalan vektorski prostor nad algebarski zatvorenim poljem k te neka je G (multiplikativan) podmonoid od $GL(E)$. Ako je E G-prost, tada je $k[G] = End_k(E)$.*

Neka je R prsten i E bilo koji R-modul. Kažemo da je E **vjeran modul** ako je zadovoljen sljedeći uvjet: Ako je $\alpha \in R$ takav da vrijedi $\alpha x = 0$ za sve $x \in E$ tada je $\alpha = 0$. U primjenama E je vektorski prostor nad poljem k te imamo homomorfizam prstena R u $End_k(E)$. U tom slučaju E je R-modul koji je vjeran ako i samo ako je dani homomorfizan injektivan.

Korolar 3.3.5. ***(Wedderburnov teorem)****. Neka je R prsten te E prost, vjeran modul nad R. Neka je $D = End_R(E)$ i pretpostavimo da je E konačnodimenzionalan nad D. Tada je $R = End_D(E)$.*

Dokaz. Neka je $\{v_1, ..., v_n\}$ baza od E nad D. Uzmimo $A \in End_D(E)$. Sad prema Jacobsonovom teoremu postoji $\alpha \in R$ takav da vrijedi

$$\alpha v_i = Av_i, i = 1, ..., n.$$

Prema tome preslikavanje $R \longrightarrow End_D(E)$ je surjekcija. Naša pretpostavka da je E vjeran modul nad R povlači injektivnost preslikavanja pa je time naš korolar dokazan. □

Primjer. Neka je R konačnodimenzionalna algebra nad poljem k te pretpostavimo da R ima jedinični element, tj. R je prsten. Ako R nema niti jedan obostrani ideal osim 0 i samog sebe, onda je svaki ne-nul modul E nad R vjeran. To nam vrijedi zato jer je jezgra homomorfizma

$$R \longrightarrow End_k(E)$$

obostrani ideal različit od R. Ako je E prost, onda je E konačnodimenzionalan nad k . Tada je i D konačnodimenzionalna algebra s dijeljenjem nad k. Wedderburnov teorem nam daje prikaz od R kao prstena D-endomorfizma od E.

Pod pretpostavkom da je R konačnodimenzionalan možemo naći prost modul uzimajući minimalni lijevi ideal različit od 0. Takav ideal postoji uzimajući lijevi ideal minimalne nenul dimenzije nad k. Još kraći dokaz Wedderburnovog teorema u ovom slučaju će biti dan u nastavku (Rieffelov teorem).

Korolar 3.3.6. *Neka je R prsten, konačnodimenzionalna algebra nad poljem k koje je algebarski zatvoreno. Neka je V konačnodimenzionalan vektorski prostor nad k sa prostom i vjernom reprezentacijom $\rho : R \longrightarrow End_k(V)$. Tada je ρ izomorfizam, tj. $R \approx Mat_n(k)$.*

Dokaz. Primijenjujemo Korolar 2.3.5. (Wedderburnov teorem). Primijetimo da je D konačnodimenzionalan nad poljem k. Neka je $\alpha \in D$. Sada vidimo da je $k(\alpha)$ komutativno potpolje od D odakle nam slijedi da je $k(\alpha) = k$ zbog pretpostavke da je k algebarski zatvoreno polje. Slijedi tvrdnja korolara. □

Primijetimo da korolar vrijedi za proste prstene, koji će biti definirani u sljedećim poglavljima.

Pretpostavimo sada da su $V_1, ..., V_m$ konačnodimenzionalni vektorski prostori nad poljem k i da je R k-algebra sa reprezentacijama

$$R \longrightarrow End_k(V_i), i = 1, ..., m,$$

odnosno V_i su R-moduli. Ako stavimo da je

$$E = V_1 \oplus ... \oplus V_m \ ,$$

dobivamo da je E konačan nad $R'(E)$ iz čega nam slijedi sljedeća posljedica Jacobsonovog teorema o gustoći.

Teorem 3.3.7. ***Egzistencija operatora projekcije.*** *Neka je k polje, R k-algebra i $V_1, ..., V_m$ konačnodimenzionalni k-prostori koji su ujedno i prosti R-moduli takvi da V_i nije R-izomorfno sa V_j za $i \neq j$. Tada postoje elementi $e_i \in R$ takvi da e_i djeluju kao identiteta na V_i i $e_i V_j = 0$ za $j \neq i$.*

Dokaz. Primijetimo da je projekcija f_i sa direktne sume E na i-ti faktor u $End_{R'}(E)$, zato jer ako je $\varphi \in R'$ onda je $\varphi(V_j) \subset V_j$, za svaki j. Prema tome možemo upotrijebiti teorem o gustoći da završimo dokaz. □

Korolar 3.3.8. ***(Bourbaki).*** *Neka je k polje karakteristike 0. Neka je R k-algebra te neka su E, F poluprosti R-moduli, konačnodimenzionalni nad k. Za svaki $\alpha \in R$, neka su α_E, α_F pripadajući k-endomorfizmi na E i F. Pretpostavimo da su im tragovi jednaki, tj.*

$$tr(\alpha_E) = tr(\alpha_F), \text{ za svaki } \alpha \in R.$$

Tada je E izomorfan sa F kao R-modul.

Dokaz. E i F su izomorfni sa konačnom direktnom sumom prostih R-modula, sa određenim multiplicitetima. Neka je V prost R - modul te pretpostavimo

$E = V^{(n)}\oplus$ direktni sumandi koji nisu izomorfni sa V.
$F = V^{(m)}\oplus$ direktni sumandi koji nisu izomorfni sa V.

Dovoljno je za dokazati da vrijedi $m = n$. Neka je e_V element u R koji zadovoljava uvjete teorema 3.3.7.. Tada vrijedi

$$tr(e_E) = n\dim_k(V) \text{ i } tr(e_F) = m\dim_k(V)$$

Kako su po pretpostavci tragovi jednaki slijedi $m = n$ s čime smo dokazali našu tvrdnju. Primijetimo da smo u dokazu koristili karakteristiku 0 jer su vrijednosti traga u k. □

3.4 Poluprosti prsteni

Prsten R nazivamo **poluprost** ako je $1 \neq 0$ i ako je R poluprost kao lijevi modul nad samim sobom.

Propozicija 3.4.1. *Ako je R poluprost prsten, tada je svaki R-modul poluprost.*

Dokaz. R-modul je kvocijentni modul slobodnog modula i slobodni modul je direktna suma od R sa samim sobom određen broj puta. Sada možemo upotrijebiti Propoziciju 3.2.2. da završimo dokaz. □

Primjeri:
1) Neka je k polje i neka je $R = Mat_n(k)$ algebra $n \times n$ matrica nad k. Tada je R poluprost, štoviše R je prost što ćemo i dokazati u poglavlju 3.5., Teorem 3.5.5..
2) Neka je G konačna grupa te pretpostavimo da karakteristika od k ne dijeli broj elemenata od G. Tada je grupni prsten $k[G]$ poluprost.

Lijevi ideal od R je R-modul za kojeg kažemo da je prost ako je prost kao modul. Dva ideala L i L' su izomorfna ako su izomorfni kao moduli.
Sad ćemo dekomponirati R kao sumu svojih prostih lijevih ideala i time dobiti strukturni teorem za R.
Neka je $\{L_i\}_{i\in I}$ familija prostih lijevih ideala u kojoj nikoja dva nisu izomorfna te takva da je svaki prosti lijevi ideal od R izomorfan jednom od tih ideala. Kažemo da je ova familija familija predstavnika izomorfnih klasa lijevih prostih ideala.

Lema 3.4.2. *Neka je L prosti lijevi ideal i E prosti R-modul. Ako L nije izomorfan sa E onda je* $LE = 0$.

Dokaz. Vrijedi $RLE = LE$ i LE je podmodul od E pa je jednak 0 ili E. Pretpostavimo da je $LE = E$. Neka je $y \in E$ takav da

$$Ly \neq 0.$$

Kako je Ly podmodul od E slijedi da je $Ly = E$. Preslikavanje $\alpha \longmapsto \alpha y$ od L u E je homomorfizam od L u E koje je surjektivno pa prema tome različito od 0. Kako je L prost, navedeni homomorfizam je izomorfizam. Dakle, L je izomorfan E, suprotno pretpostavci teorema. Slijedi $LE = 0$ □

Neka je

$$R_i = \sum_{L \approx L_i} L \,,$$

suma svih prostih lijevih ideala izomorfnih sa L_i. Iz leme zaključujemo da je $R_i R_j = 0$ ako je $i \neq j$. Vidimo da je R_i lijevi ideal te da je R suma

$$R = \sum_{i \in I} R_i$$

jer je R suma prostih lijevih ideala. Slijedi da za svaki $j \in I$ vrijedi

$$R_j \subset R_j R = R_j R_j \subset R_j.$$

Prva inkluzija vrijedi jer R sadrži jedinični element, a zadnja jer je R_j lijevi ideal. Zaključujemo da je R_j također desni ideal, tj. R_j je obostrani ideal za svaki $j \in I$.

Jedinični element 1 od prstena R možemo prikazati u obliku sume

$$1 = \sum_{i \in I} e_i$$

sa $e_i \in R_i$. Ova suma je konačna, skoro svi $e_i = 0$. Neka je $e_i \neq 0$ za indekse $i = 1, 2, ..., s$ pa pišemo

$$1 = e_1 + ... + e_s.$$

Svaki $x \in R$ možemo zapisati u obliku

$$x = \sum_{i \in I} x_i \ , \ x_i \in R_i.$$

Za $j = 1, ..., s$ vrijedi $e_j x = e_j x_j$ i

$$x_j = 1 \cdot x_j = e_1 x_j + ... + e_s x_j = e_j x_j.$$

Osim toga, $x = e_1 x + ... + e_s x$. Ovo dokazuje da ne postoji indeks i raličit od $i = 1, ..., s$ te da je i-ta komponenta x_i od x jedinstveno određena sa $e_i x = e_i x_i$. Prema tome suma $R = R_1 + ... + R_s$ je direktna te e_i je jedinični element za R_i iz čega slijedi da je R_i prsten. Kako je $R_i R_j = 0$ za $i \neq j$ imamo da je

$$R = \prod_{i=1}^{s} R_i$$

direktan produkt prstenova R_i.

Za prsten R kažemo da je **prost** ako je poluprost i ako imamo samo jednu klasu izomorfnih prostih lijevih ideala. Vidimo da smo dokazali strukturni teorem za poluproste prstene.

Teorem 3.4.3. *Neka je R poluprost. Tada postoji konačan broj ne-izomorfnih prostih lijevih ideala $L_1, ..., L_s$. Ako je*

$$R_i = \sum_{L \approx L_i} L$$

suma svih prostih lijevih ideala izomorfnih sa L_i, onda je R_i obostrani ideal koji je ujedno i prsten s operacijama naslijeđenim iz R, a R je izomorfan kao prsten sa direktnim produktom

$$R = \prod_{i=1}^{s} R_i.$$

Svaki od R_i je prost prsten. Ako je e_i jedinični element za R_i tada vrijedi $1 = e_1 + ... + e_s$ i $R_i = Re_i$. Još imamo $e_i e_j = 0$ za $i \neq j$.

Teorem 3.4.4. *Neka je R poluprost te neka je E R-modul različit od 0. Tada vrijedi*

$$E = \oplus_{i=1}^{s} R_i E = \oplus_{i=1}^{s} e_i E$$

i $R_i E$ je podmodul od E koji se sastoji od sume svih prostih podmodula izomorfnih sa L_i.

Dokaz. Neka je E_i suma svih prostih podmodula od E izomorfnih sa L_i. Ako je V prost podmodul od E tada je $RV = V$, dakle $L_i V = V$ za neki i. Prema lemi 3.4.2. imamo da vrijedi $L_i \approx V$. Dakle slijedi da je E direktna suma od $E_1, ..., E_s$. Sada je jasno da je $R_i E = E_i$. □

Korolar 3.4.5. *Neka je R poluprost. Svaki prost modul je izomorfan sa jednim od lijevih prostih ideala L_i.*

Korolar 3.4.6. *Prost prsten ima točno jedan prost modul, do na izomorfizam.*

Oba korolara su izravne posljedice Teorema 3.4.3. i 3.4.4..

Propozicija 3.4.7. *Neka je k polje i E konačnodimenzionalan vektorski prostor nad k.. Neka je S podskup od $End_k(E)$. Neka je R k-algebra generirana elementima iz S. Tada je R poluprost ako i samo ako je E poluprost R (ili S) modul.*

Dokaz. Ako je R poluprost tada je i E poluprost prema Propoziciji 3.4.1. Obrnuto, pretpostavimo da je E poluprost S-modul. Tada je E poluprost kao R-modul kao i direktna suma

$$E = \oplus_{i=1}^{n} E_i$$

gdje je svaki E_i prost. Za svaki i postoji element $v_i \in E_i$ takav da vrijedi $E_i = Rv_i$. Preslikavanje

$$x \mapsto (xv_1, ..., xv_n)$$

je R-homomorfizam iz R u E koji je injektivan kako je R sadržan u $End_k(E)$. Kako je podmodul poluprostog modula poluprost prema Propoziciji 2.2.2., slijedi tvrdnja. □

3.5 Prosti prsteni

Lema 3.5.1. *Neka je R prsten i $\psi \in End_R(R)$ homomorfizam od R u samog sebe, promatranog kao R-modul. Tada postoji $\alpha \in R$ takav da vrijedi $\psi(x) = x\alpha$ za svaki $x \in R$.*

Dokaz. Imamo $\psi(x) = \psi(x \cdot 1) = x\psi(1)$. Stavimo $\alpha = \psi(1)$. □

Teorem 3.5.2. *Neka je R prost prsten. Tada je R konačna direktna suma prostih lijevih ideala. Ne postoji niti jedan obostrani ideal osim 0 i R. Ako su L, M prosti lijevi ideali, tada postoji $\alpha \in R$ takav da vrijedi $L\alpha = M$. Imamo $LR = R$.*

Dokaz. Kako je R po definiciji poluprost slijedi da je R direktna suma prostih lijevih ideala, tj. $\oplus_{j\in J} L_j$. Možemo zapisati jedinični element u obliku konačne sume $1 = \sum_{j=1}^{m} \beta_j, \beta_j \in L_j$. Tada vrijedi

$$R = \oplus_{j=1}^{m} R\beta_j = \oplus_{j=1}^{m} L_j.$$

Ovo dokazuje našu prvu tvrdnju. Druga tvrdnja je posljedica treće. Neka je L prost lijevi ideal. Tada je i LR lijevi ideal zbog toga jer vrijedi $RLR = LR$. Kako je još i R poluprost slijedi da je LR direktna suma prostih lijevih ideala, tj.

$$LR = \oplus_{j=1}^{m} L_j \ , \ L = L_1.$$

Neka je M prost lijevi ideal. Imamo dekompoziciju u direktnu sumu $R = L \oplus L'$. Neka je $\pi : R \longrightarrow L$ projekcija koja je R - endomorfizam. Neka je $\sigma : L \longrightarrow M$ izomorfizam (postoji prema Teoremu 2.4.3.). Tada je $\sigma \circ \pi : R \longrightarrow M$ R-endomorfizam. Po lemi 3.5.1. tada postoji $\alpha \in R$ takav da vrijedi

$$\sigma \circ \pi(x) = x\alpha \text{ za svaki } x \in R.$$

Kada to primijenimo na elemente $x \in L$ dobivamo

$$\sigma(x) = x\alpha \text{ za svaki } x \in L.$$

Preslikavanje $x \mapsto x\alpha$ je ne-nul R-homomorfizam iz L u M pa je prema tome i izomorfizam. iz čega slijedi $LR = R$, čime smo dokazali naš teorem. □

Korolar 3.5.3. *Neka je R prost prsten. Neka je E prost R-modul i L prost lijevi ideal od R. Tada je LE = E i E je vjeran.*

Dokaz. Vrijedi $LE = L(RE) = (LR)E = RE = E$. Pretpostavimo da je $\alpha E = 0$ za neki $\alpha \in R$. Tada imamo $R\alpha RE = R\alpha E = 0$. Kako je $R\alpha R$ obostrani ideal vrijedi $R\alpha R = 0$ i $\alpha = 0$. Ovo dokazuje da je E vjeran. □

Teorem 3.5.4. ***(Rieffel)*** *Neka je R prsten koji nema niti jedan obostrani ideal različit od 0 i R. Neka je L ne-nul lijevi ideal, $R' = End_R(L)$ i $R'' = End_{R'}(L)$. Tada je prirodno preslikavanje $\lambda : R \longrightarrow R''$ izomorfizam.*

Dokaz. Kako je jezgra od λ obostrani ideal slijedi da je λ injekcija. Kako je također i LR obostrani ideal slijedi da je $LR = R$ i $\lambda(L)\lambda(R) = \lambda(R)$. Za svaki $x, y \in L$ i $f \in R''$ vrijedi $f(xy) = f(x)y$ zato jer je desno množenje s y R-endomorfizam od L. Stoga je $\lambda(L)$ lijevi ideal od R'' i

$$R'' = R''\lambda(R) = R''\lambda(L)\lambda(R) = \lambda(L)\lambda(R) = \lambda(R)$$

što smo htjeli i dokazati. □

Primijetimo da u Rieffelovom teoremu nismo pretpostavili da je L prost modul. S druge strane, L je ideal pa ovaj teorem nije ekvivalentan sa prijašnjim teoremima.

Kao što je istaknuto u primjeru poslije Wedderburnovog teorema, Rieffelov teorem se primijenjuje za dokaz u slučaju kada je R konačnodimenzionala algebra (sa jediničnim elementom) nad poljem k.

Sljedeći teorem nam daje obrat, pokazujući da je prsten matrica nad algebrom s dijeljenjem prost.

Teorem 3.5.5. *Neka je D prsten s dijeljenjem i E konačnodimenzionalan vektorski prostor nad D. Neka je $R = End_D(E)$. Tada je R prost i E je prost R-modul. Nadalje, $D = End_R(E)$.*

Dokaz. Prvo ćemo pokazati da je E prost R-modul. Neka je $v \in E, v \neq 0$. Tada se v može nadopuniti do baze od E nad D te stoga, uzimajući $w \in E$, postoji $\alpha \in R$ takav da vrijedi $\alpha v = w$. Stoga E ne može imati niti jedan invarijantan potprostor osim 0 i sebe samog iz čega slijedi da je E prost nad R. Također vidimo da je E vjeran nad R. Neka je $\{v_1, ..., v_m\}$ baza od E nad D. Preslikavanje

$$\alpha \mapsto (\alpha v_1, ..., \alpha v_m)$$

od R u $E^{(m)}$ je injektivan R-homomorfizam od R u $E^{(m)}$. Neka je $(w_1, ..., w_m) \in E^{(m)}$. Tada postoji $\alpha \in R$ takav da vrijedi $\alpha v_i = w_i$ pa je prema tome R R-izomorfan sa $E^{(m)}$. S ovime smo pokazali da je R (kao modul nad samim sobom) izomorfan sa direktnom sumom

prostih modula pa je prema tome poluprost. Nadalje, svi ti prosti moduli su međusobno izomorfni pa je stoga R prost prema Teoremu 3.4.3..

Ostaje nam još za dokazati da je $D = End_R(E)$. Budući da je E vektorski prostor, on je nužno i poluprost modul nad D jer očito svaki potprostor od E ima direktan komplement. Sada možemo upotrijebiti teorem o gustoći (uloge R i D su sada zamijenjene). Neka je $\varphi \in End_R(E)$ i $v \in E, v \neq 0$. Po teoremu o gustoći tada postoji element $a \in D$ takav da vrijedi $\varphi(v) = av$. Neka je $w \in E$. Tada postoji element $f \in R$ takav da vrijedi $f(v) = w$. Imamo

$$\varphi(w) = \varphi(f(v)) = f(\varphi(v)) = f(av) = af(v) = aw.$$

Slijedi da je $\varphi(w) = aw$ za svaki $w \in E$, što znači da je $\varphi \in D$ s čime smo dokazali našu tvrdnju. □

Teorem 3.5.6. *Neka je k polje i E konačnodimenzionalan vektorski prostor dimenzije m nad k. Neka je $R = End_k(E)$. Tada je R k-prostor i*

$$dim_k(R) = m^2.$$

Nadalje, m je broj prostih lijevih ideala u dekompoziciji od R na direktnu sumu.

Dokaz. k-prostor k-endomorfizma od E je prikazan kao prostor $m \times m$ matrica iz k pa je dimenzija od R kao k-prostora jednaka m^2. S druge strane u dokazu Teorema 3.5.5. pokazano je da je R R-izomorfan kao R-modul sa direktnom sumom $E^{(m)}$. Znamo da je dekompozicija modula u direktnu sumu prostih modula jedinstvena što dokazuje našu tvrdnju. □

Možemo poistovjetiti $R = End_k(E)$ sa prstenom matrica $Mat_m(k)$, kada je izabrana baza od E. U tom slučaju možemo uzeti da su prosti lijevi ideali ideali L_i $(i = 1, ..., m)$ gdje matrice u L_i imaju sve koeficijenti jednake 0 osim i-tom stupcu. Prema tome, matrica od L_1 ima sljedeći prikaz

$$\begin{pmatrix} a_{11} & 0 & \dots & 0 \\ a_{21} & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ a_{m1} & 0 & \dots & 0 \end{pmatrix}$$

Vidimo da je R direktna suma od m stupaca. Također primijetimo da nam Teorem 3.5.5. implicira sljedeće :

Ako matrica $M \in Mat_m(k)$ komutira sa svim elementima od $Mat_m(k)$ tada je M skalarna matrica.

Zaista, takva matrica M tada se može smatrati kao R-endomorfizam od E, a po Teoremu 3.5.5. znamo da takav endomorfizam leži u k.

3.6 Balansirani moduli

Neka je R prsten i E modul. Neka je $R'(E) = End_R(E)$ i

$$R''(E) = End_{R'}(E).$$

Neka je $\lambda : R \to R''$ prirodni homomorfizam takav da vrijedi $\lambda_x(v) = xv$ za svaki $x \in R$ i $v \in E$. Ako je λ izomorfizam, kažemo da je E **balansiran**. Kažemo da je E **generator** (za R-module) ako je svaki modul homomorfna slika direktne sume (moguće beskonačne) od E sa samim sobom. Na primjer, R je generator.

U Rieffelovov teoremu 3.5.4. lijevi ideal L je generator zato jer $LR = R$ implicira da postoji surjektivan homomorfizam $L \times ... \times L \to R$ pošto možemo 1 zapisati kao konačnu kombinaciju

$$1 = x_1a_1 + ... + x_na_n,\ x_i \in L \text{ i } a_i \in R.$$

Preslikavanje $(x_1, ..., x_n) \to x_1a_1 + ... + x_na_n$ je R-homomofizam lijevih modula u R.

Ako je E generator, tada postoji surjektivan homomorfizam $E^{(n)} \to R$ (možemo uzeti n konačan pošto je R konačno generiran, po jedan element 1).

Teorem 3.6.1. ***(Morita).*** *Neka je E R-modul. Tada je E generator ako i samo ako je E balansiran i konačno generiran projektor nad $R'(E)$.*

Dokaz. Dokazat ćemo pola teorema, ostavljajući drugu polovicu čitatelju. Pretpostavljamo da je E generator te dokazujemo da zadovoljava ostala svojstva teorema.

Prvo dokazujemo da je svaki modul F, $R \oplus F$ balansiran. Identificiramo R i F kao podmodule $R \oplus 0$ i $0 \oplus F$ od $R \oplus F$. Neka je $\psi_w : R \oplus F \to F$ preslikavanje definirano sa $\psi_w(x + v) = xw$, za $w \in F$. Tada svaki $f \in R''(R \oplus F)$ komutira sa π_1, π_2 i sa svakim ψ_w. Iz navedenog slijedi $f(x + v) = f(1)(x + v)$ te je stoga $R \oplus F$ balansiran. Neka je E generator i $E^{(n)} \to R$ surjektivan homomorfizam. Kako je R slobodan možemo zapisati $E^{(n)} \approx R \oplus F$ za neki modul F, tako da je $E^{(n)}$ balansiran. Neka je $g \in R'(E)$. Tada $g^{(n)}$ komutira sa svakim elementom $\varphi = \varphi_{ij}$ u $R'(E^{(n)})$ (sa komponentama $\varphi_{ij} \in R'(E^{(n)})$, stoga postoji neki $x \in R$ takav da vrijedi $g^{(n)} = \lambda_x^{(n)}$. Stoga je $g = \lambda_x$, time smo dokazali da je E balansiran kako je očito λ očito injekcija.

Da dokažemo da je E konačno generiran nad $R'(E)$ imamo da je

$$R'(E^{(n)}) \approx Hom_R(E^{(n)}, E) \approx Hom_R(R, E) \oplus Hom_R(F, E)$$

aditivna grupa. Navedena relacija očito vrijedi za R'-module ako definiramo da je operacija od R kompozicija preslikavanja (sa lijeve strane). Kako je $Hom_R(R, E)$ R'-izomorfno sa E sa preslikavanjem $h \mapsto h(1)$ slijedi da je E R'-homomorfan slici od $R'^{(n)}$, odakle nam slijedi da je konačno generiran nad R'. Također vidimo da je E direktni sumand slobodnih R'-modula $R'^{(n)}$ te je zbog toga projekcija nad $R'(E)$. Ovime završavamo naš dokaz. □

Bibliografija

[1] Lang S., *Algebra*, Springer, 2002.

[2] B. Širola, *Algebarske strukture*, https://web.math.pmf.unizg.hr/nastava/alg/predavanja/ASpred.pdf.

Sažetak

Tema ovog radu su matrice nad nekomutativnim prstenom. U prvom i drugom poglavlju pod nazivom Prsteni i Moduli uvodimo osnovne pojmove koji su nam potrebni u daljnjem dijelu rada. Pojam poluprostota, kojim se bavimo u trećem poglavlju, je najosnovniji termin koji se proteže kroz čitav diplomski rad. Prezentiramo tri definicije poluprostog modula i dokazujemo da su one ekvivalentne. Pomoću navedenih uvjetima možemo dokazati Jacobsonov teorem o gustoći te definirati pojmove poluprostog i prostog prstena. Uz Jacobsonov teorem u radu dokazujemo i druge važne teoreme, kao primjer Wedderburnov teorem koji nam daje prikaz prstena R kao D-endomorfizam nad modulom E, gdje sa D označavamo konačnodimenzionalnu algebru sa dijeljenjem nad poljem k.

Summary

The theme of this paper are matrices over noncommutative ring. In the first and second chapter titled Rings and Modules we introduce the basic concepts that are required in the far part of the work. The concept semisimlicity, the main theme of the third chapter, is the most basic term that runs through this entire graduate paper. We present three definitions of semisimple modules and prove that they are equivalent. Besides Jacobson's theorem we also prove some others very important theorems, for example Wedderbun's theorem which gives us a representation of a ring R as the ring of D-endomorphisms of module E, where D is a finite-dimensional division algebra over a field k. Using the above conditions we can prove Jacobson's density theorem and define the terms of semisimple and simple ring.

Životopis

Moje ime je Lucija Fijan. Rođena sam 09.12.1989. u Zaboku. Osnovnu školu sam završila 2004. godine u Velikom Trgovišću te iste godine upisala Prirodoslovno matematičku gimnaziju u Zaboku. Maturirala sam 2008. godine te nakon mature upisala sam Prirodoslovno-matematički fakultet, smjer Matematika, u Zagrebu . Titulu sveučilišne prvostupnice (baccalaureus) matematike stekla sam 2013. godine, te iste godine upisala diplomski studij Primijenjene matematika na istom fakultetu